Department of Homeland Security Daily Open Source Infrastructure Report for 01 March 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The United States is issuing electronic passports as part of a pilot program for diplomatic passports, and plans to issue U.S. e−passports to the American public at all domestic passport agencies by the end of 2006. (See item 22)
- ComputerWorld reports that communications remains a problem in disasters, with the complexity of modern networks making responding to a disaster not only technically difficult, but politically and culturally troublesome as well. (See item 33)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *February 28, New York Times* — **Venezuela warns it may cut back oil exports to U.S.** Venezuela's oil minister has warned that it could steer oil exports away from the U.S. and toward other markets. Venezuela is the world's fifth−largest oil exporter and supplies more than 10 percent of U.S. oil imports. The comments by minister Rafael RamÃ-rez, coupled with the increasing sale of Venezuelan oil to China, are seen by oil experts and political analysts as a signal that Venezuela is serious about finding new buyers, specifically China and India, two fast−growing, energy−hungry giants that are eager to buy Venezuelan oil. Venezuela has said that this year it will double exports to China, to 300,000 barrels a day. Venezuela ships about

1.5 million barrels a day to the U.S.
Source: http://www.iht.com/bin/print_ipub.php?file=/articles/2006/02 /27/news/venezuela.php

2. *February 28, San Francisco Chronicle* — **Storm causes widespread outages; wind gusts close to 100 mph in Bay Area.** Power was knocked out to more than 110,000 Northern California customers −− 80,000 of them in the Bay Area −− during a rainstorm Monday night, February 27, that sent wind gusts of nearly 100 miles an hour over San Francisco Bay. The power failures affected San Francisco, San Mateo, and Marin counties. The outages began around 6:30 p.m. PST and affected more than 10,000 customers in San Francisco, largely in Hunters Point and the Sunset District. The National Weather Service reported wind gusts of nearly 100 mph sweeping over San Francisco Bay, knocking down power lines, trees, and a 30−ton construction crane. On the Peninsula, the power failures affected 7,000 customers in Foster City, 5,000 customers in Millbrae, 4,700 customers in San Carlos, and 3,600 customers in South San Francisco. Flights were delayed for up to two hours at San Francisco International Airport, which was restricting landings to a single runway. Also losing power were parts of Half Moon Bay, San Mateo, Burlingame, Brisbane, and Menlo Park. An additional 30,000 Pacific Gas & Electric customers in other parts of Northern and Central California were without power.
Source: http://www.sfgate.com/cgi−bin/article.cgi?f=/c/a/2006/02/28/MNG63HFU751.DTL&feed=rss.news

3. *February 27, Financial Times (UK)* — **China needs more power.** China has underestimated the amount of new power generation it will need to meet demand, according to a Capgemini report that estimates an additional $180 billion will need to be spent by 2020. Capgemini forecasts that the country will need another 280 gigawatts (GW) of electricity generation by 2020, as well as the 950 GW planned. The report was compiled in conjunction with French utility EDF and the China Electricity Council. The China Electricity Market 2006 report says the scale of investment needed presents an opportunity for foreign investors, such as international equipment manufacturers such as GE and Alstom. Companies able to offer "clean coal" technology also have big opportunities. In spite of efforts to diversify the mix of fuels, the country will be heavily reliant on coal for its electricity, the report says. China wants to reduce the proportion of coal−fired generation from 73 percent today to less than 60 percent in 2020. However, Capgemini says coal−fired plants will still provide 71 percent of supply in 2010 and 65 percent in 2020.
Source: http://news.ft.com/cms/s/22f0e508−a735−11da−b12c−0000779e234 0.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *February 28, St. Louis Post−Dispatch* — **Tanker rupture spills gas in Missouri.** About 2,500 gallons of gasoline spilled from a ruptured tanker truck that overturned in a traffic accident near St. Louis, MO at Interstate 70 about 8 a.m. CST Monday, February 27, authorities said. St. Louis firefighters and other hazardous−material workers spent about six hours cleaning up and flushing the spill. The Metropolitan Sewer District handled the spill. A Froesel Oil Co. tanker, carrying a full load of about 10,000 gallons of gasoline, was making a turn onto I−70 and a car darted around the tanker, causing it to fall onto its side. About 2,500 gallons of gasoline spilled

out. Interstate 70 was not shut down. The reversible lanes were closed, and a portion of Broadway was closed off around the accident scene for several hours.
Source: http://www.stltoday.com/stltoday/news/stories.nsf/stlouiscityco unty/story/BF145ACBCA7D93138625712300161EDB?OpenDocument

5. *February 28, Centre Daily (PA)* — **Ammonia leak empties food plant.** An anhydrous ammonia leak in State College, PA, Monday, February 27 at Farmland Foods, 2323 S. Sheridan, forced 150 employees to evacuate and shut down a nearby street for about two hours. No injuries were reported. Chief Chuck Thomas of the Sedgwick County Fire Department said the leak occurred around 6 p.m. EST from a rooftop storage tank and was immediately shut off by an automatic safety valve. Some liquid ended up on the roof.
Source: http://www.centredaily.com/mld/centredaily/news/nation/13979 082.htm

6. *February 28, Kansas City Kansan* — **Chemical spill shuts down Kansas expressway.** The 18th Street Expressway near downtown Kansas City, KS, was shut down for several hours Monday afternoon, February 27 after a tanker truck overturned and spilled an unknown quantity of the chemical amine. The spill took place close to the intersection of 18th Street and Kansas Avenue, near the Argentine district just north of the Kansas River. Although the spill appeared to be contained, the Fire Department was taking several safety precautions.
Source: http://www.kansascitykansan.com/articles/2006/02/28/news/loc al/news2.txt

7. *February 27, Associated Press* — **Propane fire in Texas prompts evacuation.** A fire at propane company Wylie LP Gas Inc. in Lubbock, TX, blasted 5−gallon tanks into the air and as far as two blocks away on Monday, February 27. No injuries were reported. Authorities evacuated a three−quarter−mile radius after propane tanks exploded at about 4:30 p.m. CST. The cause of the explosion was not immediately clear and firefighters were working to keep a nearby 18,000−gallon tank from overheating. Lubbock fire spokesperson Mark Ethridge said the force of the explosion propelled numerous 5−gallon tanks into the air, one of which landed on the roof of a local tamale business.
Source: http://www.modbee.com/24hour/nation/story/3203850p−11919789c .html

[Return to top]

Defense Industrial Base Sector

8. *February 28, Washington Post* — **Court blocks Department of Defense's new rules for workers.** A federal judge blocked the Department of Defense (DoD) from implementing much of its new personnel system Monday, February 27. In a 77−page decision, U.S. District Judge Emmet Sullivan ruled that the Pentagon's National Security Personnel System (NSPS) fails to ensure collective bargaining rights, does not provide an independent third−party review of labor relations decisions, and would leave employees without a fair process for appealing disciplinary actions. The American Federation of Government Employees and 12 other unions representing more than 350,000 defense employees sued in November challenging the new system. Mary Lacey, program executive officer for the National Security Personnel System, said the ruling would not change the Pentagon's plans to move the first wave of 11,000 defense employees into the new pay and personnel systems at the end of April, because the rollout involves only

non−union employees, who do not participate in collective bargaining. Sullivan also ruled that the Pentagon has much broader authority to depart from standard federal labor relations systems than the unions had contended.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/02/27/AR2006022701394.html

9. *February 23, Information Week* — **Department of Defense plans to deploy RFID in operations with 24 nations.** The Department of Defense (DoD) said Thursday, February 23, it intends to move forward on plans to use active radio frequency identification (RFID) technology to support collaborative military coalition operations with 24 countries. The partner list was made final late last month. The group, including Japan, South Korea, Australia, Switzerland, and North Atlantic Treaty Organization (NATO) country members will use consistent standards to share information based on International Organization for Standards (ISO) data formats. Dan Kimball, lead technical advisor for the DoD Logistics AIT Office, said the government agency has received letters of intent from the 24 nations that intend to participate.
Source: http://www.informationweek.com/news/showArticle.jhtml?articl eID=180207549

[Return to top]

Banking and Finance Sector

10. *February 27, TechWeb News* — **PayPal password−stealing Trojan mass mailed.** Several million copies of a password−stealing Trojan horse were spammed to Internet users late last week, a security company said Monday. UK−based BlackSpider Technologies said that it had already intercepted more than 3.2 million messages with an attached Trojan, and claimed that it took 52 hours for the first anti−virus vendor to issue a signature that detected and deleted the malware. Clagger.h, as Sophos dubbed it (Symantec named it "PWSteal.Tarno.s"), comes with the subject head of "Notification: Your Account Temporally Limited," and targets PayPal users. The associated e−mail claims that PayPal has detected unusual activity on the recipient's PayPal account. If the user opens the attached file, Clagger.h silently installs. Not only does Clagger.h set a backdoor so the attacker can later add more malicious code to the PC, but it lurks in the background and nabs usernames and passwords from any window or Web page with text strings. Astute users will be waved off by a misspelling in the spam's subject heading. In the message, the word "Temporarily" is misspelled as "Temporally."
Source: http://www.techweb.com/headlines_week/showArticle.jhtml?arti cleId=181400555

11. *February 27, CNET News* — **Kits help phishing sites proliferate.** The number of phishing Websites grew by about 65 percent in December, which security experts say is due to the increasing use of easy−to−use "phishing kits." The Anti−Phishing Working Group's report for December revealed that although the number of phishing e−mails fell between November and December last year, the number of fraudulent Websites increased from 4,630 to 7,197, which is a record. The increasing number of phishing Websites can be attributed to the easy availability of phishing kits, tools that can be used by relatively non−technical people to create and manage multiple phishing sites. A similar pattern appeared several years ago when virus−making kits began appearing. According to Websense, one of the most popular phishing kits is called Rock Phish Kit.

Source: http://news.com.com/Kits+help+phishing+sites+proliferate/2100−1029_3−6043463.html?tag=cd.top

12. *February 27, Finextra* — **Alliance & Leicester to introduce two−factor authentication.** The UK's Alliance & Leicester has set out plans to introduce two−factor authentication for all Internet banking users by next month. The bank, which has over one million Internet banking customers, claims it will be "the first UK bank to roll out this type of solution to its entire Internet banking customer base."
Source: http://www.finextra.com/fullstory.asp?id=14971

13. *February 27, SC Magazine* — **FTC game teaches auction lessons.** The Federal Trade Commission (FTC) announced the launch of "Auction Action," a point−based game that teaches consumers about online fraud. The game scores users on how successfully they can answer questions about online auctions. The agency said, â€œIn 2005, the FTC received 20,450 complaints related to Internet auctions, or about 12 percent of the total number of complaints, making it the second−most common kind of complaint after those about identity theft...The new Website explains how Internet auctions work, the pros and cons of using different payment options and how −− as a buyer or seller −− you can avoid the most common types of fraud."
Game: http://www.onguardonline.gov.
Source: http://www.scmagazine.com/uk/news/article/543501/ftc−game−teaches−auction−lessons/

14. *February 27, Reuters* — **SEC shuts down $50 million Internet Ponzi scheme.** U.S. regulators last week charged the owner of 12dailypro.com and her two companies 12daily Pro and LifeClicks LLC, with fraud for running a $50 million Ponzi scheme, according to a statement released on Monday, February 27. The U.S. Securities and Exchange Commission (SEC) alleged that Charis Johnson raised more than $50 million from more than 300,000 investors by convincing visitors to the Website that they could earn a 44 percent return on their investments in 12 days by looking at Internet advertisements. The scheme, which the SEC calls "paid auto−surf," required users to buy $6 "units" −− up to a maximum of 1,000 units −− and to view advertisements from what were described as paying advertisers. While investors were led to believe that their returns would be generated by advertising revenue, payments were made almost entirely from cash generated by other unit buyers in a classic Ponzi scheme, the SEC alleged.
Source: http://www.eweek.com/article2/0,1895,1931971,00.asp

15. *February 27, Star−Bulletin (HI)* — **Bank of Hawaii e−mail scam circulates.** Officials are warning residents not to respond to a scam e−mail bearing Bank of Hawaii's name which has recently surfaced in the islands. The e−mail says, "We recently reviewed your account and we suspect an unauthorized ATM−based transaction on your account." It tells those who receive it to click on a link to a Website, where they are asked to submit personal banking information.
Source: http://starbulletin.com/2006/02/27/news/story07.html

16. *February 24, TechWeb News* — **Gaming, celebrity URLs: riskiest Websites.** In a recently published paper, researchers at the University of Washington said that some Web wards are significantly more likely to host spyware and launch "drive−by downloads," the term for the hacker practice of using browser or Windows vulnerabilities to silently install software. The

nastiest Web neighborhoods? Games and celebrity−oriented sites. In May and October 2005, Henry Levy and Steven Gribble, two University of Washington professors, sent customized Web crawlers scouring the Internet for spyware. Each foray sniffed through some 45,000 sites, then cataloged the executable files found and tested malicious sites' effectiveness by exposing unpatched versions of Internet Explorer and Firefox to drive−bys. Levy and Gribble divided the sites into ten categories that ranged from games, news, and celebrity to adult, kids, and music. One in five of gaming sites hosted spyware, said Levy and Gribble, the highest percentage of any neighborhood. Music placed second, with 11.4 percent of domains infected (about one in nine). Internet districts such as news and kids, meanwhile, were much safer. No infected news domains were spotted by Levy and Gribble, and only 1.6 percent of kids' sites hosted spyware.
Paper: http://www.cs.washington.edu/homes/gribble/papers/spycrawler .pdf
Source: http://www.informationweek.com/security/showArticle.jhtml?ar ticleID=180207761

[Return to top]

Transportation and Border Security Sector

17. *February 28, Department of Transportation* — **Atlanta Hartsfield gets $26 million pledge to help build new taxiway.** U.S. Secretary of Transportation Norman Y. Mineta on Tuesday, February 28, committed $26 million over the next five years to help Atlanta Hartsfield−Jackson International Airport build a new taxiway designed to increase safety and capacity while reducing delays. Mineta noted that the funds will be used to build an “end around” taxiway that will keep arriving flights from crossing the path of departing flights on runway 26−L as well as provide more space for departing eastbound flights to line up for takeoff. The new taxiway is expected to result in a 48 percent reduction in average delays for passengers while producing a 21 percent increase in the departure capacity of runway 26−L, he added. Mineta said Atlanta Hartsfield still has room for growth by improving traffic flow on its runways even though it already handles more than 83 million travelers and 780,000 tons of cargo each year.
Source: http://www.dot.gov/affairs/dot3404.htm

18. *February 28, Department of Transportation* — **Transportation Secretary Mineta announces pledge for South Carolina regional airport.** Department of Transportation Secretary Norman Y. Mineta on Tuesday, February 28, announced plans to spend $43 million over the next eight years to help Myrtle Beach International Airport pay for construction of an apron and new taxiways supporting the new terminal to handle growing business and attract new customers. The investment will allow the airport to accommodate up to 14 new gates by 2022 needed in anticipation of an increase in traffic at Myrtle Beach, Mineta said. He noted that improving capacity at smaller airports is vital to serving the increased number of travelers and businesses coming to the area. Myrtle Beach International Airport is one of the faster growing airports in the south handling over 785,000 passengers in 2005, an increase of almost 20,000 passengers from 2004, he said.
Source: http://www.dot.gov/affairs/dot3506.htm

19. *February 28, Department of Transportation* — **Transportation Secretary Mineta announces air travel will top one billion passengers by 2015.** Air travel will top one billion passengers a year by 2015, but the ability of the nation’s aviation system to handle the increase in traffic will depend on finding a better way to pay for airport construction and safety improvements,

Department of Transportation Secretary Norman Y. Mineta said on Tuesday, February 28, during the Federal Aviation Administration's annual forecast conference in Washington, DC. Mineta said the number of people flying has shown steady growth the past three years, surpassing record levels recorded before the September 11th, 2001 terrorist attacks. And while he called the forecast "sunny," he also warned the picture could turn bleak without reform of the federal Aviation Trust Fund. "Our growing aviation system needs a more stable and predictable revenue stream," Mineta said. Currently, trust fund revenues are collected based on a percentage of the cost of airline tickets, and have dropped in recent years due to cheaper airfares.
Source: http://www.dot.gov/affairs/dot3606.htm

20. *February 28, Associated Press* — **ATA emerges from bankruptcy.** ATA Airlines, once the nation's 10th−largest carrier, emerged from bankruptcy Tuesday, February 28, as a leaner airline that hopes to lure back passengers −− and a profit −− by focusing on vacation travel. The Indianapolis−based airline and parent company ATA Holdings have scaled back their fleet of jets, slashed destinations and cut by half their labor force since filing for Chapter 11 bankruptcy protection in October 2004. Only time will show whether ATA will be able to successfully redefine itself as a niche carrier amid turbulent economic times that have forced at least seven airlines into bankruptcy in the past three years. ATA's emergence plan −− which focuses on such destinations as Cancun, Los Angeles and Las Vegas and includes an increase in military charter business −− was approved by a federal bankruptcy judge on January30. But the keys to ATA's emergence lie in an infusion of capital from the private equity fund MatlinPatterson Global Opportunities Partners II, which agreed to invest up to $120 million, and a partnership with former low−cost rival Southwest Airlines. Under ATA's "code share" agreement with Dallas−based Southwest, passengers can buy one ticket and fly on either airline on certain routes.
Source: http://www.usatoday.com/travel/flights/2006−02−27−ata−bankru ptcy_x.htm

21. *February 27, Los Angeles Times* — **Security threat in El Monte delays travel.** Thousands of train commuters were delayed on Monday, February 27, when authorities shut down the El Monte station after a suspicious package was discovered about 5:45 a.m. PST, said spokesperson Denise Tyrrell. The bomb squad used a robot to examine the package, which appeared to be luggage. No bomb was found. Tyrrell said the package could have been mislaid by a passenger last night when trains were delayed because of a power outage.
Source: http://www.latimes.com/news/local/la−022706security_lat,0,21 84599.story?coll=la−story−footer

22. *February 27, Department of State* — **United States issuing new electronic passports in pilot program.** The United States is issuing electronic passports as part of a pilot program for diplomatic passports, and plans to issue U.S. e−passports to the American public at all domestic passport agencies by the end of 2006, the State Department has announced. According to the State Department media note on the new passports, the e−passport integrates the latest concepts in electronic document protection and readability and aims to facilitate international travel for U.S. citizens while enhancing border security. The State Department began limited production of the e−passport December 30, 2005. Officials say the e−passport is the same as a traditional passport with the addition of a small integrated circuit (or "chip") embedded in the back cover. The new passport combines face−recognition and chip technology. The chip securely will store

the same data visually displayed on the photo page of the passport (name, date of birth, gender, place of birth, dates of passport issuance and expiration, passport number), and will also include a digital photograph. The inclusion of the digital photograph will enable biometric comparison, through the use of facial recognition technology at international borders, officials say. In addition, the State Department also has included basic access control technology in the new passports to prevent skimming and eavesdropping.
Source: http://usinfo.state.gov/gi/Archive/2006/Feb/27−535.html?chan lid=globalissues

[Return to top]

Postal and Shipping Sector

23. *February 28, Yahoo! bizjournals* — **UPS rebrands Overnite as UPS Freight.** United Parcel Service Inc. has renamed Overnite Corp., which it bought in 2005 for $1.3 billion, UPS Freight. UPS said the subsidiary's workers will sport new uniforms and drive newly branded trucks starting May 1. The facilities and fleet, including 22,000 trailers, will be rebranded to UPS Freight over the next several years, UPS officials said. UPS Freight will continue to operate independently of the UPS package delivery network. UPS Freight will consist of three main service categories: UPS Freight LTL, UPS Freight Truckload, and Specialty Solutions. Atlanta−based UPS provides package delivery services to more than 200 countries and territories. The company bases its UPS Airlines division at Louisville International Airport.
Source: http://biz.yahoo.com/bizj/060228/1233990.html?.v=3

24. *February 27, CBS4 News* — **Explosive scare at Sunrise post office.** An explosive scare at a South Florida post office on Monday, February 27, led to an evacuation and shutdown. The Sunrise Post Office, just off Hiatus Road, was shutdown for two hours when a van caught fire in the parking lot and became completely engulfed in flames. CBS4 reports the van was converted into some type of camper powered by a small propane tank.
Source: http://cbs4.com/local/local_story_058130839.html

[Return to top]

Agriculture Sector

25. *February 28, Texas Agriculture* — **State animal health commission delays premise identification ruling.** Hearing complaints ranging from privacy invasion to infringement of certain religious practices, Texas animal health officials opted to delay ruling on the proposed premise identification plan pending further review. Once approved, the Premise ID plan will require landowners to register with the state the types of animals kept on a particular piece of property. Bob Hillman, Texas State Veterinarian, said Premise ID involves providing Texas Animal Health Commission (TAHC) with a contact name, phone number, physical address, and the types of animals housed, managed or otherwise handled on a piece of property, such as a ranch, veterinary clinic, arena, or livestock market. Roughly 7,000 of the roughly 200,000 farms in Texas have already registered with TAHC, all under voluntary compliance measures currently available. Premise ID is the first in a series of steps needed for what TAHC said will be a national animal identification system that allows health officials to better identify, track

and ultimately, contain and treat animal disease outbreaks when they occur.
Source: http://www.txfb.org/TexasAgriculture/2006/030306/030306anima lID.htm

26. *February 28, Southeast Farm Press* — **Early thrips numbers high in Georgia.** Thrips, tiny insects that can carry a deadly crop disease, have weathered south Georgia's winter better than usual. Thrips can get the tomato spotted wilt virus (TSWV) from an infected plant when they are nymphs. When they get older, they can carry the disease to other plants as they feed. The severity of the disease can vary from year to year. Over the past two decades, TSWV has cost Georgia farmers hundreds of millions of dollars in damage to crops like peanuts, tobacco, peppers, and tomatoes. A female thrips can produce five to 90 more female thrips. Each can reach maturity in about two weeks and produce another five to 90 more.
Source: http://southeastfarmpress.com/news/022806−Georgia−thrips/

[Return to top]

Food Sector

27. *February 27, Animal and Plant Health Inspection Service* — **French poultry banned due to highly pathogenic avian influenza.** The U.S. Department of Agriculture's (USDA) Animal and Plant Health Inspection Service (APHIS) has placed a temporary ban on the importation of poultry and commercial shipments of live birds, hatching eggs, and unprocessed avian products from the French Department (state) of Ain based on the diagnosis of highly pathogenic avian influenza H5N1 in commercially raised turkeys. The ban became effective February 25. The restriction is only on the Department of Ain, not the entire country of France. Previously, USDA has placed bans on the following countries due to the presence of the H5N1 strain of avian influenza in commercial flocks: Cambodia, Egypt, India, Indonesia, Japan, Laos, Kazakhstan, Malaysia, Nigeria, China, Romania, Russia, South Korea, Thailand, Turkey, Ukraine, and Vietnam. Processed poultry products from these countries must be accompanied by a USDA permit. Permits are issued by APHIS' Veterinary Services. They confirm that the products were treated according to government requirements.
Source: http://www.aphis.usda.gov/newsroom/content/2006/02/frenchai_vs.shtml

[Return to top]

Water Sector

28. *February 28, North Jersey Media Group* — **France buys parent of United Water.** The parent of United Water, North New Jersey's biggest water supplier, is being sold to a utility holding company controlled by the French government. State−backed Gaz de France SA on Monday, February 27, said it would buy energy and water supplier Suez SA for more than $46 billion in cash and stock. The deal was finalized over the weekend. United Water, which started in 1869 as the Hackensack Water Co., owns water systems throughout the U.S. Its United Water New Jersey unit delivers water to 1.2 million residents. Because the full structure of the sale was not announced, it was uncertain whether the deal will require formal approval from the New Jersey Board of Public Utilities.
Source: http://www.northjersey.com/page.php?qstr=eXJpcnk3ZjczN2Y3dnF

lZUVFeXkyOSZmZ2JlbDdmN3ZxZWVFRXl5Njg4ODU1OSZ5cmlyeTdmNzE3Zjd2cWVlRUV5eTI=

29. *February 28, Journal News (NY)* — **More radioactivity detected in Indian Point water.** Federal nuclear regulators plan to inspect new samples of underground water at Indian Point Tuesday, February 28, after the New York nuclear plants' owner said that tiny amounts of radioactive tritium and strontium−90 appear to be seeping into the Hudson River. Both radioactive isotopes are byproducts of nuclear reactor operations, but federal regulators and local emergency officials say there is no threat to public safety now because the levels detected were near or below amounts allowed for safe drinking water. Company and public officials say both radioactive materials could be coming from a leak in the 400,000−gallon, 40−foot−deep spent−fuel pool near Indian Point 2, which was found during excavation work at the site in August. Company officials said the leak never reached more than two liters a day, was quickly contained and has since stopped. They have not, however, ruled out that the pool has other leaks or the possibility that the water moving underground now might have been trapped more than a decade ago during an earlier leak.
Source: http://www.thejournalnews.com/apps/pbcs.dll/article?AID=/20060228/NEWS09/602280361/1025

[Return to top]

Public Health Sector

30. *February 28, Agence France−Presse* — **German cat gets H5N1 bird flu, virus spreads.** Germany reported the first known case in Europe of H5N1 bird flu infecting a cat. The dead cat was found on the Baltic Sea island of Ruegen, where the highly pathogenic form of H5N1 bird flu was detected mid−February, said Germany's national veterinary laboratory, the Friedrich Loeffler Institute. In the bird population, the disease was spreading further across Europe and Africa. France began vaccinating 700,000 domestic ducks and geese on farms after it announced the first outbreak of H5N1 bird flu in a European Union poultry farm. Sweden for the first time detected in ducks an unidentified strain of bird flu, feared to be the H5N1 strain. Initial tests at Sweden's the National Veterinary Institute "show that we're probably talking about the same virus that has been spreading in Russia and China," said the Swedish agriculture board. Elsewhere, H5N1 was detected for the first time in Bosnia, the southern German state of Bavaria, and a poultry farm in southwestern Russia where 103,000 birds were reported to have died in a week. Ethiopian officials were testing some of more than 6,000 chickens that died suddenly on a poultry farm in Endibir. In Nigeria H5N1 was detected in two more states in the north.
Source: http://news.yahoo.com/s/afp/20060228/hl_afp/healthfluworld_0 60228160311

31. *February 28, Knight Ridder Newspapers* — **New Orleans hospitals overflowing.** New Orleans, LA's strained hospitals reached the breaking point Monday, February 27, as Mardi Gras reveling neared its peak. New Orleans' only two functioning emergency rooms were overflowing and they told authorities they couldn't accept new patients. Hospitals in nearby Jefferson Parish were also dangerously full. That means more of a burden on MED−1, the mobile emergency room from Charlotte, NC, that is serving as a de facto hospital for New Orleans during Mardi Gras. The New Orleans metro area had 5,200 hospital beds before

Katrina. With several of the major hospitals flooded and closed, that's dropped to 1,800 beds. Most were full even before the weekend's influx of people for Mardi Gras. Helicopters are standing by to fly people to hospitals in Baton Rouge and Shreveport, if needed.
Source: http://www.kansascity.com/mld/kansascity/news/nation/1397814 9.htm

32. *February 28, United Press International* — **Hantavirus kills U.S. airman.** Intensive cleaning is under way at U.S. military−range housing in New Mexico in the wake of the hantavirus death of an Arizona serviceman. Senior Airman Leonard Hankerson Jr., who was with the 56th Security Forces Squadron at Luke Air Force Base, AZ, died February 11 at Texas' Beaumont Army Medical Center.
Hantavirus information: http://www.cdc.gov/ncidod/diseases/hanta/hps/index.htm
Source: http://upi.com/NewsTrack/view.php?StoryID=20060228−110033−23 64r

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

33. *February 27, ComputerWorld* — **Communications still a problem in disasters, experts say.** The complexity of modern communications networks, both wired and wireless, makes responding to a modern−day disaster not only technically difficult, but politically and culturally troublesome as well, said Andrew Lippman, director of the Massachusetts Institute of Technology Media Lab. Lippman was part of a roundtable discussion in Cambridge, MA, that included communications experts from government and the private sector. Panelists acknowledged that enormous communications obstacles still exist, including the need for widespread adoption of interoperable radios for emergency first responders. That task alone could take years to complete.
Source: http://www.computerworld.com/mobiletopics/mobile/story/0,108 01,109046,00.html

[Return to top]

Information Technology and Telecommunications Sector

34. *February 28, BBC News (UK)* — **Viruses plague British businesses.** Computer viruses are the single biggest cause of security problems for UK businesses, a survey by the Department of Trade and Industry (DTI) shows. Almost 50 percent of the biggest security breaches in the last two years were due to malicious programs. Viruses crippled key systems such as e−mail for more than a day while companies cleaned up, and the worst outbreaks sometimes took up to 50 days to fix. The survey revealed that the number of firms affected by viruses had dropped by almost one−third since 2004. This reduced infection rate is due to the of use anti−virus software. The survey found that firms that do get caught tend to get infected far more often; some were being infected once a day. Almost 25 percent of those surveyed said they had no

defenses to protect them against spyware. As a result one in seven of the most serious incidents were caused by machines infected with spyware. The DTI survey questioned more than 1,000 businesses. The full results of the survey will be released in April.
Source: http://news.bbc.co.uk/2/hi/technology/4755492.stm

35. *February 28, CNET News* — **Oracle patches 11i security flaws.** Oracle has issued an upgrade to its E−Business Suite 11i diagnostics module containing a number of the security fixes, according to applications security firm Integrigy. Oracle made an unusual move by alerting its users about the security patches, according to Integrigy's advisory. Historically, Oracle has released product upgrades but not disclosed whether they included security fixes, Integrigy noted. The "Diagnostics Support Pack February 2006 with Oracle Diagnostics 2.3 RUP A" aims to address security flaws in Oracle diagnostics Web pages and Java classes, according to Integrigy. "The significant (security) issue is (that) some diagnostics can be executed without any authentication, and it is possible to configure the diagnostics to be unrestricted," according to the Integrigy report. Although the company releases quarterly security updates, "Oracle has not previously provided customers a notification that security fixes were included (in an upgrade)," Integrigy noted in its report.
Source: http://news.com.com/Oracle+patches+11i+security+flaws/2100−1002_3−6044020.html?tag=cd.lede

36. *February 27, Government Computer News* — **IRS needs to tighten security settings.** The IRS has not consistently maintained the security settings it established and deployed under a common operating environment (COE), resulting in a high risk of exploitation for some of its computers, according to the Treasury Departmentâ€™s inspector general for tax administration (TIGTA). The IRS has adopted a common operating environment for security configurations on all of its workstations. The IRS has installed the master COE image on 95 percent of its computers, TIGTA said in its report released Monday, February 27. Of 102 computers tested, only 41 percent continued to be in compliance; 59 percent were not or contained at least one high−risk vulnerability that would allow the computer to be exploited or rendered unusable. Almost one−half of the compliant computers contained at least one incorrect setting that could allow employees to circumvent security controls established by the common operating environment. Also, at the time of the audit, the COE security settings had not been installed on more than 4,700 computers. Without them, computers were missing security patches and at high risk for viruses.
Report: http://www.ustreas.gov/tigta/auditreports/2006reports/200620 031fr.pdf
Source: http://www.gcn.com/vol1_no1/daily−updates/38341−1.html

37. *February 27, ComputerWorld* — **Breaches push companies to improve internal safeguards; security managers shift focus to preventing accidental data leaks.** After spending years implementing controls to protect network perimeters from external threats, companies are now guarding against internal data lapses, according to attendees at RSA Conference 2006 this month. Driving the trend are concerns about accidental data leaks or thefts resulting from internal miscues, a rash of recent data breaches caused by the mishandling of information, and regulations that require companies to exercise greater control over data they handle. "Even up to last year, there was a huge focus on strengthening the perimeter to make sure the hacker from outside didn't get in," said Stuart McIrvine of IBM. "Everyone was concerned about malware penetrating the perimeter." More recently, though, "there's been a big shift in focus to what's

going on inside the enterprise," McIrvine said. Gene Fredriksen of Raymond James Financial Inc. said "Traditional information security has been very good at protecting structured data." But now, he added, there's a whole class of unstructured data in spreadsheets, Web forms, and other formats.
Source: http://www.computerworld.com/printthis/2004/0,4814,109007,00 .html

38. *February 27, SC Magazine* — **Cross−infecting virus discovered.** The first malware to cross−infect a PC and a Windows wireless pocket device has been discovered, the Mobile Antivirus Researchers Association (MARA) said. The proof−of−concept, file−destroying Trojan automatically spreads from a Win32 desktop to a Windows Mobile Pocket PC. "With the growing use of hand−held devices, this type of virus may become very prevalent in the futureâ€¦ This virus closes the gap between handhelds and desktops," the association said. Jonathan Read of MARA said that previous "crossover" viruses −− "required either Bluetooth on the device and the PC, or the user had to physically transfer the virus on a memory card." But this trojan is the first to use ActiveSync −− a program that synchronizes files and other data between a Windows PC and a Windows Mobile device −− to cross−infect a desktop and hand−held PC. It also is the first crossover malware to infect the PC before attacking the mobile device. Dave Cole, director of Symantec Security Response, said today that he expects hackers to continue to experiment with new platforms, such as mobile devices. He predicts such attacks gradually will become more financially motivated as users increase their reliance on hand−held computers in their daily lives.
Source: http://www.scmagazine.com/uk/news/article/543503/crossinfect ing−virus−discovered/

39. *February 26, WSYR News Channel 9 (NY)* — **Digital phone outage spans New York.** Thousands of Time Warner Digital Phone customers lost service Sunday afternoon, February 26. Time Warner blames the outage on a software glitch. Time Warner says at 1:45 p.m. EST Sunday the digital phone system crashed. For two hours, every customer in New York State was without phone service before service was restored.
Source: http://www.9wsyr.com/news/local/story.aspx?content_id=c1d482 9a−46cc−4ab0−8dd6−a0e52c1ed3cd&rss=112

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of publicly available exploit code for a vulnerability in Apple Safari Browser. The Apple Safari browser will automatically open "safe" file types, such as pictures, movies, and archive files. A system may be compromised if a user accesses an HTML document that references a specially crafted archive file. Successful exploitation may allow a remote, unauthenticated attacker to execute arbitrary commands with the privileges of the user.

More information can be found in the following US−CERT Vulnerability Note:

VU#999708 − Apple Safari may automatically execute arbitrary shell commands
http://www.kb.cert.org/vuls/id/999708

Although there is limited information on how to fully defend against this exploit, US−CERT recommends the following mitigation:

Disable the option "Open 'safe' files after downloading," as specified in the Securing Your Web Browser document.

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 25 (smtp), 445 (microsoft−ds), 139 (netbios−ssn), 41170 (−−−), 80 (www), 22159 (−−−), 21838 (−−−), 113 (auth) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.

Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer